MONTHLY TECHNICAL REPORT

DoD PKI MIGRATION TO OPEN STANDARDS

November 1999

Prepared By:

Defense Information Systems Agency
JIEO Center For Information Technology Standards

TABLE OF CONTENTS

1. OVERVIEW

This technical report contains an October/November 1999 summary of ongoing analyses performed on PKI-related products for conformance to standards, and to evaluate the PKI standards themselves for suitability to DoD requirements. This work is being conducted in the Standards Analysis Facility (SAF) at Ft. Monmouth, NJ by the Network Applications and Security Branch of the DISA Center For Information Technology Standards (CFITS). The SAF supports testing of the DoD PKI server environment to related commercial vendor products including:

- Netscape End-Entity (EE) applications;
- Microsoft (MS) EE applications;
- Lotus EE applications;
- MS PKI-enabled Server applications;
- Lotus PKI-enabled Server applications;
- Federal PKI MISPC Reference Implementation;
- LDAP vendor products;
- S/MIME vendor products.

2. DOD PKI STANDARDS EVALUATIONS

2.1 BACKGROUND

The SAF has set up within a DoD PKI Test Environment in order to support the current DoD PKI implementation. This support consists of evaluating the developing suite of PKI standards generated by: the Internet Engineering Task Force (IETF); the Federal Government; the DoD; and ancillary standard groups. Closely related to this work is: evaluating the most widely used vendor products that are being used in DoD networks; examining PKI capabilities of new software that will eventually be introduced into the DoD network; and determining how well the DoD PKI implementation conforms to the required standards.

The DoD PKI Test Environment is a mirror of the technology used in the Pilot DoD PKI consisting of: a Root Certificate Authority (CA); two each intermediate Identify (ID) and E-mail CAs; associated Directory Servers (DSs); multiple web servers; a Domain Name Service (DNS) server; POP3 and IMAP mail servers; and multiple client machines. The client machines are all MS Windows NT-based and either has MS Windows NT 4 Server with Service Pack 4 or MS Windows NT 5 (Beta) Server loaded. The server machines are UNIX-based Sun Workstations with the Common Operating Environment (COE) as a foundation loaded with an image of the currently fielded Pilot DoD PKI software.

2.2 ANALYSIS

This month's PKI standards analysis focused on the following areas:

- Summary and cross-comparison of standards conformance tables of the DoD PKI, Microsoft, Lotus, and NIST MISPC implementations;
- S/MIME standards and associated commercial products.

2.3 PKI STANDARDS CONFORMANCE SUMMARY TABLE

To date, evaluations have been performed on the DoD PKI V1, Microsoft Windows 2000 Beta, and the NIST MISPC PKI Reference Implementation. An evaluation on Lotus V5 (Domino, Notes) has been completed and is included in the attached table (Appendix B) that compares the results of evaluating the four products. This table was assembled in order to allow easy comparison of the four products.

As described at the top of the table and described in previous reports, the baseline for the tables is the DoD Medium Assurance Functional Specification, V0.3, dated 20 October 1998. Sections of the document that define hard technical requirements and reference underlying standards produced by the IETF and ISO were put in a table format. The wording of the Specification's technical sections were analyzed, then the products were evaluated for conformance. In some cases determining conformance was straight forward. In other cases a best guess approach had to be taken due to the product's inability to present information that would answer the questions.

Each product had to be evaluated according to the functional roles defined for PKI components including Certification Authority (CA), Directory Services, Registration Authorities, and end users(EE). (Note that Directory Services were nested under CA, and Registration Authorities were nested under EE). The table breaks these components out only into CAs and EEs for simpler reading. All of the products were evaluated for their full capability in supporting CA, DS, RA, and EE functions.

The resulting table shows the obvious that the DoD PKI V1 is almost fully conformant to the Specification, while the other three products vary in conformance. Microsoft Windows 2000 Beta showed relatively close conformance with the only general area showing negative in Certificate Types. This was only due to not configuring the system to support these specialized certificate types. Lotus V5.1 Domino and Notes do not support the X.509 extension, nor CRLs. In communicating with Lotus technical staff, these features should be implemented in their V5.2 release. The NIST MISPC implementation shows the least conformance, due to its construction as only a Reference Implementation, its limited functionality (e.g. SSL not supported) and its tracking with the Federal standards supporting different algorithms (DSS instead of RSA).

Work will be ongoing in this effort with the goal of developing these tables as a means of evaluating conformance of a given product against both commercial standards and specific DoD requirements for PKI. Another set of tables has been developed which track with the accepted and emerging IETF standards defining PKI technology. These tables, much more detailed than the one that tracks with the DoD Functional Specification, are planned for use when the situation calls for a deeper level of analysis.

[At this point the four product analyses and the underlying conformance table are still in draft form. Comments/Corrections would be greatly appreciated].

2.4 S/MIME STANDARDS ANALYSIS

Work has just started in this area. The focus is on evaluating the emerging S/MIMEv3 standards for fit to DoD requirements for secure mail. The research will be based on the IETF standards defining S/MIMEv3. Efforts to date include the development of conformance tables for these four protocols and the acquisition of a S/MIMEv3 Reference Implementation (RI) obtained from J G Van Dyke, which is currently being loaded within the SAF. Van Dyke developed the RI for NSA use and for use by vendors to develop email applications that meets S/MIMEv3 standards. The code must be compiled before use and has been successfully compiled within the SAF. Status at this point is determining the capabilities and user interface of the executable software in order to determine an evaluation plan.

2.4.1 General

The work for the month of October has been broken into three areas of study:

1. Review and parsing of S/MIME v3 IETF RFC's to extract specific requirements.
2. Determine the availability of S/MIME v3 products.
3. Develop a plan for the evaluation of S/MIME v3 products against the RFC's to determine if the products meet the requirements of the DOD.

The overall goal of this initial work is to: a) Determine the specific S/MIME v3 requirements; and b) Have a plan in place to that COTS products can be evaluated as they are available.

2.4.2 SMIME RFC's

The IETF S/MIME Working Group has completed five Proposed Standards that comprise the S/MIME version 3 specification. Following is a list of these RFC's along with the current status of parsing the requirements:

1. RFC 2630, Cryptographic Message Syntax - TBD
2. RFC 2631, Diffie-Hellman Key Agreement Method – Small RFC
3. RFC 2632, S/MIME Version 3 Certificate Handling – Nearly complete
4. RFC 2633, S/MIME Version 3 Message Specification – Completed July 12, 1999
5. RFC 2634, Enhanced Security Services for S/MIME – 50 % Complete

In addition to the RFC's there are several Internet Drafts under study in the S/MIME working groups. These Internet Drafts currently include the following:

a) Certificate Distribution Specification
b) Domain Security Services using S/MIME
c) Examples of S/MIME Messages
d) Methods for Avoiding the 'Small-Subgroup' Attacks on the Diffie-Hellman Key Agreement Method for S/MIME
e) Incorporation of IDEA encryption algorithm in S/MIME
f) CMS KEA and SKIPJACK Conventions Password-based Encryption for S/MIME
g) Use of the CAST-128 Encryption Algorithm in S/MIME Elliptic Curve S/MIME

2.4.3 S/MIME Products

We know of no commercially available S/MIME v3-capable email clients at this time. However, there is a lot of prototyping in progress and the major vendors are in the process of upgrading their S/MIME products to include v3 capabilities.

2.4.4 Product Evaluation Plan

During October, work continued investigating the Van Dyke S/MIME Freeware Library (SFL) to determine if the tool could be used to support product evaluation against S/MIME requirements. In addition to reviewing the SFL, a meeting was held to "brainstorm" potential methodologies to evaluate the S/MIME products as they become available. First, the October experience with SFL is summarized.

S/MIME Freeware Library (SFL) Investigation

Based on our continuing difficulties to successfully compile and run the reference implementation test programs in the SFL, we requested further help from Van Dyke and Associates, the developers of SFL. At the same time we identified ourselves as DISA/JIEO. Van Dyke responded promptly with the suggestion that they would supply us with a full copy of their development environment except for the BSAFE libraries (from RSA). They also implied that this version would be configured to build and test just the Free3 CTIL. Subsequent to this exchange, the promised development environment continued to experience problems. The following list briefly describes our activities and observations:

- It was observed that this copy appears to be version 1.2 while the version available from the web site is still at 1.1.
- An examination of the directory structure revealed differences in placement of key subdirectories.

- Loading the project into the MS VC IDE generated the warning that the subproject file for the “snacc.dll” was missing, i.e., this is not a complete copy of the development environment.
- The libraries were built and “auto_hid.exe” was built and run. This produced an error that the command line arguments were missing.
- Adding command line parameters to the project (per pervious messages from Van Dyke) allowed the program to run, producing two apparently non-fatal errors: “decode past end of data”; before it ended with the same “dll load” message we had seen before.
- Attempted to build the project “sm_rsaDLL” with the same results as before, i.e., “missing a global”.
- Investigation of the RSA web site revealed a number of BSAFE products with varying version numbers. It is not clear from the SFL documentation which library is required.
- Examination of the directory reveals several new test configuration files and differences between the web site distribution and the files from Van Dyke.

As a result of the continuing difficulties with the compilation and running of the SFL reference implementation we made contact with the chief SFL developer at Van Dyke by phone. The following are some of the key points from the conversation.

- SFL is a complex development environment and Van Dyke has a dedicated team of developers, who have been there of some period of time, working full time on the effort.
- We identified the proper test configuration file and were able to successfully run the SFL reference tests for the first time.
- They explained the test environment portion of the SFL, e.g., the tests driven by the configuration files, are in fact a unit test environment intended primarily for the use of the Van Dyke development staff.
- They confirmed that there is no written documentation on the command structure of the configuration files but he reviewed some of the basics with us.

As discussed above, the test files were developed to be used by the SFL developers. Therefore, the output would provide the developer with feedback on the code that the developer is very familiar with. For the output to be meaningful for others, they would need to go through the uncompiled C++ code, following the nested config files, to determine the meaning of the output. Therefore, using the SFL test configuration files as a component of the S/MIME v3 product evaluations would require an in-depth understanding of the overall SFL development environment.

Based on our experience with the code and conversations with Van Dyke, we decided to take a step back and review various options for evaluating the S/MIME products. The first option would be to develop “simple” S/MIME-enabled mail application based on the SFL Programming APIs to use in lieu of the test environment. We are still in the process of scoping this option to develop a reasonable resource estimate.

Plans for Evaluating Products

At this time, our technical support (AT&T) is investigating potential alternative methodologies for evaluating the S/MIME products as they become available. One of the ideas suggested included using various v2 and v3 products set up a test suite whose components could be configured to emulate specific requirements. Another idea was to narrow down the requirements to the set that specifies the features of special interest to the DoD.

Sources for DoD PKI requirements included *SDN.701: Message Security Protocol (MSP) 4.0* as one document that would likely contain a large set of the Government PKI messaging requirements. Shortly thereafter, we obtained copies of the viewgraphs presented by the S/MIME Working Group at the 1999 RSA conference. These viewgraphs confirmed that a combination of *RFC 2630 Cryptographic Message Syntax* and *RFC 2634 Enhanced Security Services for S/MIME* document a protocol that provides equivalent security features as MSP 4.0.

APPENDIX A: GLOSSARY

a.k.a.	Also Known As
CA	Certificate Authority
CFITS	Center for Information Technology Standards
COE	Common Operating Environment
COTS	Commercial off the Shelf
DDK	MS Driver Developers Kit
DER	Distinguished Encoding Rules
DII	Defense Information Infrastructure
DNS	Domain Name Server
DS	Directory Server
IE4	Microsoft Internet Explorer 4.01
IE5	Microsoft Internet Explorer 5 (BETA)
IETF	Internet Engineering Task Force
IP	Internet Protocol
SAF	Standards Analysis Facility (DISA Ft. Monmouth, NJ)
LDAP	Lightweight Directory Access Protocol
MMC	Microsoft Management Console
NT4	Microsoft NT 4
NT5	Microsoft NT 5 (BETA)
.p7c	Cryptographic Message Syntax Standard – PKCS#7
PC	Personal Computer
.pfx/.p12	Personal Information Exchange – PKCS#12
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
POP3	Post Office Protocol 3
RA	Registration Authority
RAM	Random Access Memory
Sigverif	Signature Verification Utility
SP4	Service Pack 4 (Microsoft released Nov 98)

APPENDIX B

Date: 5 November 1999

Products under Evaluation:

1) DoD PKI V1
2) Microsoft Windows 2000 Beta
3) Lotus Domino/Notes Version 5.1
4) NIST MISPC Implementation

for compliance to the DOD Medium Assurance PKI Functional Specification, v0.3, 20 OCT 98.

Compliance codes: Y - System supports requirements
N - System does not support requirement
P - System partial supports requirement
A - Analysis pending

Requirement	Reference	DoD PKI	MS 2000	Lotus V5	NIST MISPC	Comments
General		CA|EE	CA|EE	CA|EE	CA|EE	
Configurable Parameters	3.1.1	Y | Y	Y | Y	Y | Y	P | P	
SSL	3.1.2	Y | Y	Y | Y	Y | Y	N | N	
Confidential Administrative Communications	3.1.3	Y | Y	Y | Y	Y | Y	P | P	
Certificate Fields		CA|EE	CA|EE	CA|EE	CA|EE	
Version 3 Support	3.2.1.1	Y | Y	Y | Y	Y | Y	Y | Y	
Serial Number	3.2.1.2	Y | Y	Y | Y	Y | Y	Y | Y	
Signature	3.2.1.3	Y | Y	Y | Y	Y | Y	Y | Y	
Issuer	3.2.1.4	Y | Y	Y | Y	Y | Y	Y | Y	
Validity	3.2.1.5	Y | Y	Y | Y	Y | Y	Y | Y	
Subject	3.2.1.6	Y | Y	Y | Y	Y | Y	Y | Y	
Subject Public Key Information	3.2.1.7	Y | Y	Y | Y	Y | Y	Y | Y	
Issuer Unique Identifier not used	3.2.1.8	Y | Y	Y | Y	Y | Y	Y | Y	
Subject Unique Identifier not used	3.2.1.9	Y | Y	Y | Y	Y | Y	Y | Y	
Issuer's Signature	3.2.1.11	Y | Y	Y | Y	Y | Y	Y | Y	
Certificate Extensions		CA|EE	CA|EE	CA|EE	CA|EE	
Authority Key Identifier	3.2.2.1.1	Y | Y	Na | Y		N | Y	

Requirement	Reference	DoD PKI	MS 2000	Lotus V5	NIST MISPC	Comments
Subject Key Identifier	3.2.2.1.2	Y | Y	Y |Na		Y | Y	
Key Usage: Digital Signature	3.2.2.1.3	Y | Y	Y | Y		N | N	
KU: Non-repudiation	3.2.2.1.3	Y | Y	Y | Y		N | N	
KU: Key Encipherment	3.2.2.1.3	Y | Y	Na | Y		N | N	
KU: Key Certificate Signature	3.2.2.1.3	Y | Na	Y | Na		N | N	
KU: CRL Signature	3.2.2.1.3	Y | Na	Y | Na		N | N	
Private Key Usage Period not used	3.2.2.1.4	Y | Y	Y | Y		Y | Y	
Certificate Policies	3.2.2.1.5	Y | Y	N | N		Y | Y	
Policy Mapping not used	3.2.2.1.6	Y | Y	Y | Y		Y | Y	
Subject Alternative Names	3.2.2.2.1	N | N	Na | Y		N | N	
Issuer Alternative Names	3.2.2.2.1	N | N	Na | Y		N | N	
Subject Directory Attributes not used	3.2.2.2.2	Y | Y	Y | Y		Y | Y	
Basic Constraints	3.2.2.3	Y | N	Y | N		Y | N	
Name Constraints	3.2.2.3	N | N	N | N		Y | Y	
Policy Constraints	3.2.2.3	P | P	N | N		Y | Y	
CRL Distribution Points	3.2.2.4.1	Y | Y	Y | Y		Na | N	
Signing Algorithms		CA|EE	CA|EE	CA|EE	CA|EE	
RSA	3.2.3.1	Y | Y	Y | Y	Y | Y	N | N	
DSS	3.2.3.2	N | N	A | A	? | ?	Y | Y	
Certificate Types		CA|EE	CA|EE	CA|EE	CA|EE	
Root CA	3.2.4.1.1	Y | Na	Y | Na	N | N	P | Na	
Signing CA	3.2.4.1.2	Y | Na	Y | Na	N | N	Y | Na	
Identity	3.2.4.2.1	Y | Y	Na | Y	N | N	Y | Y	
E-mail	3.2.4.2.2	Y | Y	Na | Y	N | N	N | N	
Server	3.2.4.2.3	Y | Y	Na | Y	N | N	N | N	
Developer	3.2.4.2.4	Y | Y	Na | Y	N | N	N | N	
Enabled Device	3.2.4.2.5	Y | Y	Na | Y	N | N	N | N	
Certificate Revocation List (CRL) Fields		CA|EE	CA|EE	CA|EE	CA|EE	
Version 2	3.3.1.1	Y | Na	Y | Na	N	Y | Na	
Issuer Name	3.3.1.2	Y | Na	Y |	N	Y | Na	
This Update	3.3.1.3	Y | Na	Y |	N	Y | Na	
Next Update	3.3.1.4	Y | Na	Y |	N	Y | Na	
Revoked Certificates	3.3.1.5	Y | Na	Y |	N	Y | Na	
CRL Extensions		CA|EE	CA|EE	CA|EE	CA|EE	
Authority Key Identifier	3.3.2.1	N | Na	Y | Na	N	N | Na	
Issuer Alternative Name	3.3.2.2	Y |	Y |	N	Y | Na	

Requirement	Reference	DoD PKI	MS 2000	Lotus V5	NIST MISPC	Comments
not used						
CRL Number	3.3.2.3	Y |	N |	N	N | Na	
Issuing Distribution Point	3.3.2.4	Y |	N |	N	N | Na	
Delta CRL Indicator	3.3.2.5	Y |	N |	N	Na|Na	
CRL Entry Extensions		CA|EE	CA|EE	CA|EE	CA|EE	
Reason Code: Unspecified not used	3.3.3.1	N | Na	P | Na	N	Y | Na	
RC: Key Compromise	3.3.3.1	N | Na	Y | Na	N	Y | Na	
RC: CA Compromise	3.3.3.1	N	Y | Na	N	Y | Na	
RC: Affiliation Changed	3.3.3.1	N	Y | Na	N	Y | Na	
RC: Superseded	3.3.3.1	N	Y | Na	N	Y | Na	
RC: Cessation of Operations	3.3.3.1	N	Y | Na	N	Y | Na	
RC: Certificate Hold not used	3.3.3.1	N	Y | Na	N	N | Na	
RC: Remove from CRL	3.3.3.1	N	N | Na	N	Na|Na	
Expiration Date not used	3.3.3.2	Y	Y | Na	Y	Y | Na	
Instruction Code not used	3.3.3.3	Y	Y | Na	Y	Y | Na	
Invalidity Date	3.3.3.4	N	N | Na	N	N | Na	
Certificate Issuer	3.3.3.5	N	N | Na	N	Y | Na	
Directory Schema		CA|EE	CA|EE	CA|EE	CA|EE	
Directory Hierarchy	3.4.1	Y	Y | Na	Y	Y | Na	
Distinguished Names	3.4.2	Y	Y | Na	Y	Y | Na	
CA Directory Objects	3.4.3.1	Y	Y | Na	N	Y | Na	
Individual Directory Objects	3.4.3.2	Y	Y | Na	N	P | Na	
Country Object	3.4.3.3	Y	Y | Na	Y	Y | Na	
Organization Objects	3.4.3.4	Y	Y | Na	Y	Y | Na	
Organizational Unit Objects	3.4.3.5	Y	Y | Na	Y	P | Na	
PKI Roles Objects	3.4.3.6	Y	Y | Na	Na	N | Na	
Device Objects	3.4.3.7	Y	A | Na	N	Na|Na	
Processes		CA|EE	CA|EE	CA|EE	CA|EE	
Identification, Authentication and Access Control of CA Personnel	3.5.1.1	Y	Y | Na	N	P | Na	
Identification, Authentication and Access Control of RA Personnel	3.5.1.2	Y	P | Na	N	Y | Na	
Identification, Authentication and Access	3.5.1.3	Y	P | Na	N	N | Na	

Requirement	Reference	DoD PKI	MS 2000	Lotus V5	NIST MISPC	Comments
Control of LRA Personnel						
Identification, Authentication and Access Control of Subscribers	3.5.1.4	Y	Y | Na	N	Y | Na	
Identity Certificate Authorization, Request and Issue	3.5.2.1	Y	Y | Y	Y	N | Na	
Email Certificate Authorization, Request and Issue	3.5.2.2	Y	Y | Y	N	N | Na	
Other Certificate Authorization, Request and Issue	3.5.2.3	Y	Y | Na	N	Y | Na	
Disabling Pre-Authorizations	3.5.2.4	Y	Y | Na	N	N | Na	
Processing Authorizations	3.5.2.5	Y	Y | Na	Y		
Certificate Renewal and Reissue	3.5.3	Y	Y | Na	Y	Y | Na	
Certificate Expiration	3.5.4	Y	Y | Na	Y	Y | Na	
Certificate Revocation	3.5.5	Y	Y | Na	N	Y | Na	
CRL Management	3.5.6	Y	Y | Na	N	Y | Na	
Certificate Removal	3.5.7	Y	Y | Na	Y	Y | Na	
Key Generation	3.5.7.1	Y	Y | Na	Y	P | Na	
Key Recovery and Key Protection	3.5.8	Y	Y | Na	Y	N | Na	
System Configuration	3.5.9.1	Y	Y | Na	Y	Y | Na	
CA Management	3.5.9.2	Y	Y | Na	Y	P | Na	
Key Management	3.5.9.3	Y	Y | Na	N	P | Na	
User Role Management	3.5.9.4	Y	Y | Na	Y	Y | Na	
System Administrator	3.5.9.5	Y	Y | Na	Y	Y | Na	
CA Staff	3.5.9.6	Y	Y | Na	N	P | Na	
RA	3.5.9.7	Y	Y | Na	N	Y | Na	
LRA	3.5.9.8	Y	Y | Na	N	N | Na	
Audit Logs	3.5.10	Y	Y | Na	N	P | Na	
Archive	3.5.11	Y	Y | Na	N	P | Na	
Interfaces		CA|EE	CA|EE	CA|EE	CA|EE	
User Web Interface for Certificate Request	3.6.1.1.1	Y	Y	Y	N | N	
User Web Interface for Certificate Issue	3.6.1.1.2	Y	Y	Y	N | N	
User Web Interface for	3.6.1.1.3	Y	Y	Y	N | N	

Requirement	Reference	DoD PKI	MS 2000	Lotus V5	NIST MISPC	Comments
Directory Search						
System Administrator Interface	3.6.2.1	Y	Y	Y	N | N	
CA Staff Interface	3.6.2.2	Y	Y	N	N | N	
RA Interface	3.6.2.3	Y	N	N	N | N	
LRA Interface	3.6.2.4	Y	N	N	N | N	

Comments: